Applications of Automated Deduction to Problems in Group Axiomatics

William McCune

Mathematics and Computer Science Division
Argonne National Laboratory

Outline of OTTER

- OTTER is a resolution/paramodulation deduction system.
  - applies to statements in first-order logic with equality
  - searches for proofs
  - emphasizes fast deduction (indexing)
  - can also be used as a symbolic programming system
- OTTER is not completely automatic.
  - the user decides on inference rules and search strategies
  - the user usually interacts by running a sequence of jobs

Inference Rules of OTTER

The inference rules operate on clauses.

- Resolution rules
  - binary resolution
  - hyperresolution
  - unit-resulting (UR) resolution
- Paramodulation
- Demodulation (term rewriting)

Search Strategies of OTTER

- Deciding where to start the search.
- Selecting the next clause for application of inference rules.
  - simplest-first, breadth-first, user-defined weight function, or a combination of these.
- Deciding whether to keep inferred clauses.
  - discard complex clauses
  - discard clauses with "bad" terms
- Orienting equations and adding new rewrite rules
  - Lexicographic Recursive Path Ordering (LRPO)
  - user-defined weight functions
  - deciding which orientable equations should be rewrite rules.

Strengths and Weaknesses

- Strengths
  - Small Theories
  - Hyperresolution on Horn sets or Near-Horn sets
  - UR-resolution on Horn sets or Near-Horn sets
  - Paramodulation with unit clauses and demodulation (including Knuth-Bendix completion)
  - Use as a symbolic programming system
  - Otter is general-purpose
- Weaknesses
  - Rich theories
  - Non-Horn sets
  - "If-and-only-if" definitions
  - Working with many Skolem functions
  - No case analysis
  - Otter is general-purpose

Status of OTTER and Other Automated Deduction Software at Argonne

- Version 2.2 of OTTER was released in July 1991.
  - is available by anonymous FTP and is included in the second edition of *Automated Reasoning: Introduction and Applications*
- Prototype theorem provers
  - ROO, the parallel (shared-memory) version of OTTER, with John Slaney of Australian National University
  - SCOTT, semantically constrained OTTER, also with Slaney
- We have written new code for associative/commutative (AC) matching and unification.
  - Performance is good, especially for AC matching.
  - Indexing for AC matching.
  - We are starting to experiment with AC paramodulation.

FINite Domain EnumeratoR

(by John Slaney, Australian National University)

- Searches for small (finite) models of first-order statements.
- We used FINDER to find counterexamples—for example, to find a model of a candidate single axiom that is not associative.

Applications to Axiomatic Group Theory

- General problem: given an axiom system, find equivalent but simpler systems, including (if possible) single axioms.
- Our focus: find simple single axioms for varieties of group theory.
  - general groups, Abelian groups, Boolean groups, exponent groups
  - with standard operators (product, inverse, identity), with nonstandard operators (division, double division), and various combinations.
  - restricted to equational theories
- This requires theorem-*finding* as well as theorem-proving.
  - given a set of equations E, find a simple equation $\alpha = \beta$ in the theory of E such that $\alpha = \beta \Rightarrow E$.

Groups in Terms of Product and Inverse

The standard axiomatization of groups (e is the identity):

(1a)	$e \cdot x = x$
(1b)	$x \cdot e = x$
(2a)	$x^{-1} \cdot x = e$
(2b)	$x \cdot x^{-1} = e$
(3)	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

However, {1a,2a,3} is sufficient, and {1b,2b,3} is sufficient.

- B. H. Neumann's single axiom for groups (1981)
  $(x \cdot (((y^{-1} \cdot (x^{-1} \cdot z))^{-1} \cdot u) \cdot (y \cdot u)^{-1})^{-1}) = z$
  - Note that it does not contain the identity e; in fact, there is no single axiom in terms of product, inverse, and identity (Tarski).
- First goal: to find a simpler single axiom
  - measures: length, number of variables, and number of variable occurrences.

Construct a Set of Candidates

- Start with identities up to some bound on length.
- Then Reduce the set to a manageable size (< 5000).
  - by theory—for example,
    (1) if $\alpha = \beta$ is a single axiom, then either α or β is a variable;
    (2) if inverse is present, it must have an odd number ≥ 3 number of occurrences.
  - by intuition—for example, use candidates that are similar to known single axioms.
- Or apply transformations to an existing set of candidates.

Construct a Set of Candidates (cont'd)

Otter was "programmed" to do various tasks, for example:

- Construct all binary associations of a string.
- Given term t, construct $\{t' | t'$ can be obtained from t by inserting one occurrence of $e\}$.
- Given a set of equations, rewrite each with $x^{-1} = x \cdot x \cdot x$; then paramodulate one level from the left argument of $x \cdot x \cdot x \cdot x = e$.
- Given a set of equations, generate 10,000 consequences of the set; then extract equations with three distinct variables and one occurrence of e.

Try Each Candidate

- Fix the search strategy and automatically run a sequence of OTTER jobs, one with each candidate.
  - Search based on Knuth-Bendix completion.
  - Allow non-orientable equations to participate in the search.
  - Limit the size of equations in the search.
  - Combine simplest-fist and breadth-first search when selecting the next equation for application of paramodulation.
  - Forward search (mostly)—use negated equations (goals) only to detect proofs.
  - Input many goals—known single axioms and elements of multi-equation axiomatizations.
- Run each OTTER job for a minute or so, and collect the proofs that were found.

Success!

- A single axiom with 2 fewer occurrences of inverse: $(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u$

  (and 213 others of the same size)

- Open question
  - Is there a single axiom (for groups in terms of product and inverse) of this size in just 3 variables?
  - (Ken Kunen has shown that a single axiom must have at least this many applications of product, and at least this many applications of inverse.)

OTTER Can Find Complex Proofs Quickly

Theorem 1. *The theory of groups can be defined by the single axiom*

$$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u. \tag{3.1}$$

Proof. First, Eq. (3.1) holds in groups, a fact that can be checked by straightforward calculation. Next, consider the following derivation, starting with (3.1).

5	$(x \cdot (y \cdot (((z \cdot z^{-1}) \cdot (u \cdot y)^{-1}) \cdot x))^{-1}) = u$	[(3.1)]
7	$(x \cdot ((((y \cdot y^{-1}) \cdot (z \cdot u)^{-1}) \cdot (v \cdot v^{-1})) \cdot (z \cdot x))^{-1}) = u$	[5→5]
9	$(x \cdot ((y \cdot (z \cdot z^{-1})) \cdot (u \cdot x))^{-1}) = (((v \cdot v^{-1}) \cdot (y \cdot u)^{-1}) \cdot (w \cdot w^{-1}))$	[5→7]
10	$(((y \cdot y^{-1}) \cdot (((z \cdot z^{-1}) \cdot (u \cdot x)^{-1}) \cdot u)^{-1}) \cdot (v \cdot v^{-1})) = x$	[7→9]
12	$(((x \cdot x^{-1}) \cdot y^{-1-1}) \cdot (z \cdot z^{-1})) = y$	[10→10]
14	$((x \cdot x^{-1}) \cdot (y \cdot z)^{-1}) = ((u \cdot u^{-1}) \cdot (y \cdot z)^{-1})$	[10→5]
15	$((x \cdot x^{-1}) \cdot y^{-1}) = ((z \cdot z^{-1}) \cdot y^{-1})$	[12→14:12]
17	$(u \cdot u^{-1}) = (v \cdot v^{-1})$	[15→5:5]
19	$(x \cdot x^{-1}) = ((y \cdot y^{-1}) \cdot (z \cdot z^{-1})^{-1})$	[17→15]
20	$(((x \cdot x^{-1}) \cdot ((y \cdot y^{-1}) \cdot z)^{-1}) \cdot (u \cdot u^{-1})) = z^{-1}$	[17→10]
22	$(x \cdot (y^{-1} \cdot ((z \cdot z^{-1}) \cdot x))^{-1}) = y$	[17→5]
25	$(x \cdot ((u \cdot u^{-1})^{-1-1} \cdot (w \cdot x))^{-1}) = w^{-1}$	[19→7:20]
32	$((x \cdot x^{-1})^{-1} \cdot (y^{-1} \cdot (z \cdot z^{-1}))^{-1}) = y$	[17→22]
34	$(x^{-1} \cdot ((y \cdot y^{-1})^{-1-1} \cdot (z \cdot z^{-1}))^{-1}) = x^{-1}$	[17→25]
36	$((y \cdot y^{-1}) \cdot (x \cdot (z \cdot z^{-1})^{-1-1})^{-1})^{-1} = x$	[5→25]
44	$(x \cdot ((y \cdot y^{-1})^{-1-1} \cdot (z \cdot z^{-1}))^{-1}) = x$	[36→34:36]
48	$((x \cdot x^{-1})^{-1-1} \cdot (y \cdot y^{-1})) = (z \cdot z^{-1})$	[44→17]

52	$(x \cdot (y \cdot y^{-1})^{-1}) = x$	[48→44]
57	$((z \cdot z^{-1})^{-1} \cdot u)^{-1-1} = u$	[52→10:20]
62	$(x^{-1} \cdot (y \cdot y^{-1}))^{-1} = x^{-1-1}$	[32→57]
65	$(y \cdot ((z \cdot z^{-1}) \cdot (x \cdot y)^{-1}))^{-1} = x^{-1-1}$	[5→57:52]
76	$(x \cdot (y \cdot y^{-1}))^{-1} = x^{-1}$	[57→62:57]
88	$((x \cdot x^{-1})^{-1} \cdot y^{-1-1}) = y$	[65→32]
92	$((u \cdot u^{-1}) \cdot y^{-1})^{-1} = y$	[65→20:12,76]
116	$(y \cdot (u \cdot u^{-1})) = y$	[76→32:76,88]
126	$((y \cdot z) \cdot z^{-1}) = y$	[76→5:92]
201	$(x \cdot y^{-1-1}) = (x \cdot y)$	[126→126]
207	$((x \cdot x^{-1}) \cdot z) = z$	[19→126:52,201]
215	$(x \cdot (y \cdot ((x \cdot y)^{-1} \cdot u))) = u$	[5→126:207,201]
227	$y^{-1-1} = y$	[126→36:207,52]
229	$(z \cdot x)^{-1} = (x^{-1} \cdot z^{-1})$	[126→25:227,207]
239	$(x \cdot ((x^{-1} \cdot u) \cdot y)) = (u \cdot y)$	[126→5:207,229,229,227,227]
260	$((x \cdot y) \cdot z) = (x \cdot (y \cdot z))$	[215→215:229,229,229,227,227,239]

By 17, there exists a unique element e such that for all x, $(x \cdot x^{-1}) = e$; it follows from 116 that e is a right identity; and 260 shows the associativity of product. ∎

Abelian Groups in Terms of Product and Inverse

- B. H. Neumann's single axiom (1981): $(((x \cdot y)^{-1} \cdot (y \cdot x))^{-1} \cdot ((z \cdot u)^{-1} \cdot (z \cdot ((v \cdot w^{-1}) \cdot u^{-1})^{-1})))^{-1} \cdot w = v$
- New single axiom: $((x \cdot y) \cdot z) \cdot (x \cdot z)^{-1} = y$

Group Axioms in Terms of Division

- General groups in terms of division, $\alpha/\beta = (\alpha \cdot \beta^{-1})$:

  $(x/((((x/x)/y)/z)/(((x/x)/x)/z))) = y$

  [Higman and Neumann 1952]

- Abelian groups in terms of division:

  $(x/(y/(z/(x/y)))) = z$ [Tarski 1938]

We found other axioms of the same type, but none simpler.

Other Combinations of Operations

- Double division: $\alpha \parallel \beta = \alpha^{-1} \cdot \beta^{-1}$.
- We found new single axioms for each of the following combinations:

	General	Abelian
double division, identity	Simpler*	First
double division, inverse	First	First
division, identity	First**	First
division, inverse	First**	First

* Neumann presented a single axiom for general groups in terms of double division and identity (1986); the new single axiom is simpler.

** Tarski showed (1968) that axioms exist, but none was given.

Exponent Groups (work with Larry Wos)

- Groups in which x^n is the identity, for all x.
- An axiomatization with identity (x^n is right-associated):

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	associativity
$e \cdot x = x$	left identity
$x^n = e$	exponent property

- An axiomatization without identity:

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	associativity
$y^n \cdot x = x$	left identity
$x^n = y^n$	exponent property

- Boolean groups ($n = 2$)
  - Single axioms without identity were known, e.g., $x \cdot ((y \cdot z) \cdot (x \cdot z)) = y$.
  - Single axioms with identity were easy to find, e.g., $((x \cdot y) \cdot (z \cdot y)) \cdot (x \cdot e) = z$.

Exponent Groups Without Identity

- Exponent 3: consider all associations of $xxxyzzz = y$. Single axioms discoved include

$$x \cdot ((x \cdot (x \cdot (y \cdot (z \cdot z)))) \cdot z) = y \quad (4.2)$$
$$x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot (z \cdot z)) = y \quad (4.3)$$
$$x \cdot ((((x \cdot x) \cdot (y \cdot z)) \cdot z) \cdot z) = y \quad (4.4)$$

- Exponent 4: failure.
- Exponent 5: consider associations of $xxxxyzzzz = y$. Results include

$$x \cdot (x \cdot ((x \cdot (x \cdot (x \cdot (y \cdot (z \cdot (z \cdot (z \cdot z))))))) \cdot z)) = y \quad (4.5)$$
$$x \cdot (x \cdot ((x \cdot (x \cdot ((x \cdot y) \cdot z))) \cdot (z \cdot (z \cdot (z \cdot z))))) = y \quad (4.6)$$

- Consider (4.2) and (4.5), note similarity, and conjecture axioms for exponents 7 and 9:

$x(xxyzz)z = y$	exponent 3	(4.2)
$xx(xxxyzzzz)z = y$	exponent 5	(4.5)
$xxx(xxxxyzzzzzz)z = y$	exponent 7	(4.7)
$xxxx(xxxxxyzzzzzzzz)z = y$	exponent 9	(4.8)

- OTTER quickly proved the conjectures. We then proved (by hand) that the pattern works for all odd exponents.
- Results with identity were similar.

Single Axioms for Even Exponents

- are much more difficult to find for exponents > 2.
- We have several for exponent 4 with identity, for example,

  $x \cdot ((e \cdot ((x \cdot (x \cdot ((x \cdot (y \cdot z)) \cdot z))) \cdot z)) \cdot z)) = y$
  $x \cdot ((x \cdot ((e \cdot ((x \cdot (x \cdot (y \cdot z))) \cdot z)) \cdot z)) \cdot z)) = y$
  $x \cdot ((x \cdot ((x \cdot ((e \cdot ((x \cdot y) \cdot z)) \cdot z)) \cdot z)) \cdot z)) = y$
  $x \cdot ((e \cdot ((x \cdot ((x \cdot ((x \cdot y) \cdot z)) \cdot z)) \cdot z)) \cdot z)) = y$

  (Note curious nesting property.)
- For exponent 4 without identity, we can replace e with w^4 to obtain single axioms, but we have not found any with 10 variable occurrences.
- For even exponents > 4, we have not found any single axioms in product and identity or in product alone.

Other Work on Single Axioms with Automated Deduction

- These are excellent test problems for evaluating new programs and approaches.
- Kalman, Winker, and Wos (~1980) answered several open questions on whether particular formulas are single axioms for various logic calculi.
- The first single axioms for non-equality axiomatizations of groups were found with methods (McCune 1991) similar to the work presented here.
- Motivated by our work, Ken Kunen found new and simpler (by one measure) axioms by using OTTER.
  - considered general groups with product and inverse
  - used models to give lower bounds on form of single axioms